German IT Security Law

John A. Foulks*

This country brief is meant to give the reader an overview of the history and present status of IT security regulation in Germany. It follows a chronological organization, covering the period from 1991 through the end of 2017. The German federal parliament, the Bundestag, began updating and expanding the mandate of the Federal Office for Information Security (the *Bundesamt für Sicherheit in der Informationstechnik* – the "BSI") in 2015. Generally, the aim has been to secure critical infrastructure, defined in terms of public access to a list of basic services and necessities, from vulnerabilities due to the ubiquitous use of information technology. The European legislation behind the most recent set of German enactments is introduced in turn. The presentation finishes by identifying a foreseeable European-level regulation of cybersecurity product certification for the single European market, as well as the establishment of the European Union Agency for Network and Information Security ("ENISA") as the pan-European cybersecurity agency. The article may serve as an introduction and a starting point for more in-depth research. It identifies and summarizes major substantive provisions of the respective enactments and regulations over time. It also

* *John A. Foulks* is an alumnus of Dartmouth College, Indiana University and, since 2017, Rutgers Law School. Through Rutgers, he attended the international exchange program at Bucerius Law School in Hamburg in 2016. He joined the JLCW editorial staff in 2017. John is currently a Chancery Division law clerk at New Jersey Superior Court and is admitted to practice in New Jersey. He has been living in Germany or working with German in one way or another nearly nonstop since 1994, including studying, teaching, and translating.

offers assorted insights into the legislative history. The subject matter is presented in abridged form. In general, it was necessary to dispense with many details, in particular when it came to minute legislative tweaks to existing law in several areas in order to accommodate new cybersecurity regulations.

I. CREATION OF THE FEDERAL OFFICE FOR INFORMATION SECURITY (THE BSI)

The BSI, a subordinate agency within the Federal Ministry of the Interior (*Bundesministerium des Inneren* – the "BMI"), is Germany's national cybersecurity authority. It is tasked with "shap[ing] information security in digitization through prevention, detection and reaction for government, business and society."[1] The BSI was established almost three decades ago, by way of legislation that took effect in 1991.[2] The legislation that called the BSI into existence defined "information technology" as any technological means of distributing or transferring information, and "security" as the observance of standards to ensure the availability, integrity or confidentiality of information. The means of achieving security were to be found within IT systems and components, and in the ways such systems and components were used.[3] At the time, the

---

[1] *Das BSI*, BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, http://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz_node.html (last visited Mar. 5, 2018) (Ger.).

[2] Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik [BSI-Errichtungsgesetz] [BSI Formation Act], Dec. 17, 1990, BGBL I at 2834, as amended by Art. 11 of the Verordnung [V] [Regulation] of Nov. 25, 2003, BGBL I at 2304 (Ger.).

[3] *See id.* § 2.

Bundestag charged the new BSI with investigating security risks associated with the use of IT and developing preventive measures, in the form of security processes and devices. The BSI was also charged with developing criteria, processes, and tools for testing and evaluating the security of IT systems and components, and carrying out that testing and evaluation.[4]

With certain exceptions, the 1991 law expressly limited the scope of the BSI's activity to securing the IT-related applications of the German federal government.[5] It could, however, provide security advice to manufacturers, merchants and users of IT, in particular regarding the risks associated with using such IT equipment.[6] By way of background to the most recent developments (through 2017), it bears emphasis that the 1991 Act provided that manufacturers and merchants of IT systems should be able to apply to the BSI for certification of their products.

The BSI was empowered to grant IT product security certification on two broad conditions. The first was that systems and components should fulfill generally recognized criteria, or criteria established by the BSI. The second condition was that the BMI (the BSI's parent agency) had to determine that no federal security or preponderating public interests weighed against certification.[7] Security certificates from other "recognized" agencies in the European Community were to be recognized by the BSI if such certificates demonstrated an "equivalent security" level.[8] As of the end of 2017, the member-state-specific product certification regimes now in place let product cybersecurity

[4] *See id.* § 3(1) nos. 1 – 3.
[5] *See id.* § 1(1) no. 1; §§ 4 – 6.
[6] *See id.* § 3(1) no. 7.
[7] *See id.* § 4.
[8] *See id.* § 4(4).

certifications be recognized across member states pursuant to a small number of multilateral agreements among subsets of EU member states.[9] These appear likely to be displaced or preempted in the foreseeable future as the European Commission has issued a proposed regulation on the topic.[10]

II. MAJOR OVERHAUL OF THE BSI STATUTE IN 2009

In 2009, the Bundestag passed very significant amendments by way of an act styled as one "to increase the security of the IT of the federal government."[11] The act (hereinafter "the BSIG of 2009") expanded the set of defined terms to refer to "communications technology operated by federal authorities as well as its interfaces,"[12] with "interfaces" further defined according to the official English translation[13] as "security-relevant gateways within federal communications technology and between this technology and the information technology of individual federal

---

[9] *Commission Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency," and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")*, at 1, COM (2017) 477 final (Sept. 13, 2017), https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en.

[10] *Id.*

[11] Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes [BSIG] [Act on the Federal Office for Information Security], Aug. 14, 2009, BGBL I, 54, at 2821-26, *translation at* https://www.gesetze-im-internet.de/englisch_bsig/index.html (Ger.) [hereinafter BSIG of 2009]. As of February 2018, the cited English translation does not reflect substantial subsequent amendments; however, the German text at the same location does. See the amending acts cited below at notes 31 & 65.

[12] *Id.* § 2(4).

[13] *See* BSIG of 2009, *supra* note 11.

authorities, groups of federal authorities, or third parties."[14] New definitions also included harmful software, security gaps or flaws, protocol data and data transmissions.[15] Only a selection is cited here. The amended definitions alone indicate the expanded scope of the law precipitated by the 2009 amendments.

The tasks delegated to the BSI multiplied accordingly. The BSI was now responsible for defending against threats as well as collecting and analyzing information about security risks and measures.[16] Further, it was tasked with operating cryptographic and security management systems for other agencies of the federal government, and with testing and advising on these systems.[17] The BSI retained its former advisory role but was now also charged with issuing warnings to German federal and state entities, private manufacturers, merchants and users of IT concerning the security thereof.[18] Furthermore, the BSI was charged with establishing suitable communication channels for purposes of timely recognizing, reacting to, and overcoming crises affecting critical *information* infrastructure.[19]

The BSI's reach and responsibility was thus limited because of the way the Bundestag had defined its mission. Instead of mandating that the BSI safeguard critical

---

[14] BSIG of 2009, *supra* note 11, § 2(3), (4), at 2821. Note the carve-outs for IT operated by the other constitutional organs, namely the two federal legislative houses, *Bundestag* [federal parliament] and *Bundesrat* [federal council], the *Bundesrechnungshof* [the independent federal auditing agency] and the federal courts.
[15] *Id.*
[16] *Id.* § 3(1) no. 2.
[17] *Id.* § 3(1) nos. 8, 9, at 2822.
[18] BSIG of 2009, *supra* note 11, § 3(1) no. 14, at 2822.
[19] *Id.* § 3(1) no. 15, at 2822 (emphasis added).

infrastructure, presuming (as we must) that IT produces a new set of vulnerabilities anywhere it is used, the Bundestag at the time tasked the BSI with reacting to and overcoming crises affecting critical *information infrastructure* only. The good to be protected was thus conceived of narrowly. But it has since become obvious that infrastructure in general has been made to depend on computerized information, and it is no longer possible to observe the ubiquity and scale of information and be content to secure only *its* infrastructure. Subsequent amendments have addressed the formerly inadequate scheme. Whether they have done so well has been the subject of debate both within the Bundestag, as well as between it and the government, in advance of the subsequent amendments discussed below.

Still, the associated principles of cybersecurity survived the subsequent paradigm shift. The 2009 overhaul of the BSI's mandate called for the agency to coordinate a cooperative effort with private industry, albeit with the express, relatively narrow aim of protecting the good referred to in limited fashion as critical information infrastructure.[20] The BSIG of 2009 overall not only greatly expanded the role of the BSI at the time but also still embodies the primary crystallization of the current approach. Section 4 of the BSIG of 2009 established the BSI as the "central clearinghouse"[21] for cooperation among German federal agencies on IT security. The BSI was tasked with observing and evaluating attacks against IT systems and informing federal agencies of attacks.[22] Reciprocally, the new law obligated other federal agencies to communicate

[20] *Id.*

[21] *Id.* § 4, at 2822. Again note that the English translation published as of this writing does not reflect substantial further amendments enacted in 2015 and 2017.

[22] *Id.* § 4(2).

relevant information to the BSI should it come to the other agencies' attention first.[23] The BSI was also empowered to assist the German states, upon their request, with securing their own IT.[24]

The BSIG imposed certain limits on the BSI's activities were also imposed, and these have also survived subsequent amendments. It has been a source of continual controversy that individually identifiable data collected by the BSI acting under its cyber security mandate could be available to various other security or law enforcement agencies. The limits imposed on the BSI therefore involve administrative and judicial oversight around data protection issues.

For one thing, the 2009 amendments expressly preserved the norms otherwise applicable to handling personally identifiable information.[25] In operating federal communications technology, and at the "interfaces" of such technology as defined above,[26] communications protocol data would foreseeably accumulate. Whether and how such data was permitted to be automatically analyzed or retained was made to depend upon a series of conditions. If communication protocol data contained personally identifiable information or data that was subject to the norms governing secrecy in telecommunications, then the extent of automated analysis was limited to what was required to recognize, isolate and eliminate disturbances, and to defend against malicious software.[27] The generally permitted automated analysis just described had to occur right away; and such data could not be retained at all after the stated

[23] *Id.* § 4(3).
[24] *Id.* § 3(2), at 2822.
[25] BSIG of 2009, *supra* note 11, § 4(5), at 2823.
[26] *Id.* § 2(4).
[27] *Id.* § 5(1).

objective had been accomplished.[28] Non-automated use of the data, or use in a way that would associate it with particular persons, was permissible only under a further series of detailed restrictions. Not automated use of the data had to be supported by a reasonable suspicion arising from particularized facts. Moreover, the scope of the authority to analyze such data was limited to what was required to confirm or allay suspicion of, and to defend against, malicious software.[29] Affected persons had to be informed of non-automated analysis of the data. Rights related to data protection and core personal privacy interests were to be respected unless the government could satisfy a number of conditions all involving oversight by federal agents charged with data protection, or by the courts.[30]

III. THE 2015 AMENDMENTS TO THE BSIG

The BSIG received its next major overhaul just roughly six years later on July 17, 2015.[31] According to the BSI, the 2015 enactment expanded the agency's role with the aim of bolstering IT security of critical infrastructure beyond the administrative boundaries of the federal government.[32] The legislative materials state that the basic motivation for the enactment was to better protect the authenticity, availability, confidentiality and integrity of IT systems for businesses, citizens' online activity, and the BSI and *Bundeskriminalamt* (the Federal Criminal Police

---

[28] *Id.*
[29] *Id.* § 5(2), 5(3).
[30] *Id.* § 5(4) – (7).
[31] IT-Sicherheitsgesetz [IT Security Act], July 17, 2015, BGBL I, 31, at 1324–31 (Ger.).
[32] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, *supra* note **Error! Bookmark not defined.**.

Office).[33]

Generally referred to as the IT Security Act, the 2015 amendments appointed the BSI as a threat sharing agency if not in terms, then at least in effect.[34] This follows from the legislative materials: the Bundestag sought to obligate operators of critical infrastructure to adhere to a set of minimum standards for cybersecurity and to notify the BSI in the event of cybersecurity incidents.[35] With the BSI continuously disseminating intelligence gathered from all operators of critical infrastructure, a given operator supposedly would reap more in return than it had provided, in the form of better information and know-how about threats.[36] The Bundesrat's position document asserts that the IT Security Act observed the basic principle behind the European Commission's then-proposal, enacted later by the European Union as the NIS Directive.[37]

The document offering the draft legislation[38] sought

---

[33] *See, e.g.*, Gesetzentwurf der Bundesregierung [Cabinet draft], Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) [Draft of an Act to Increase the Security of IT Systems – IT Security Act], Dec. 29, 2014, BUNDESRAT DRUCKSACHEN [BR] 643/14 at 2, https://www.bundesrat.de/SharedDocs/drucksachen/2014/0601-0700/643-14.pdf (Ger.) [hereinafter BR 643/14]; *see also* Gesetzentwurf der Bundesregierung [Cabinet draft], Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) [Draft of an act to increase the security of IT systems – IT Security Act], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 18/4096 at 19, http://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf (Ger.) [hereinafter BT 18/4096].

[34] *See id.*

[35] *Id.*

[36] *Id.*

[37] BR 643/14, *supra* note 33, at 3.

[38] BT 18/4096, *supra* note 33.

to recognize that telecommunications providers are one key to cybersecurity. They would be obligated to maintain state of the art IT security in order to meet the legal standards for telecommunications secrecy as well as to secure personally identifiable information and the availability of their own services. The Bundesnetzagentur (Federal Network Agency), otherwise charged with overseeing telecommunications markets,[39] would handle law enforcement aspects as well as the obligatory notification of the BSI in the event of cyber incidents. The verbal standard "state of the art" has been controversial, as discussed below.

The IT Security Act's provisions were detailed and numerous.[40] Significantly, this legislation amended the phrase "critical information infrastructure" in section 3(1), second sentence, no. 15 of the BSIG, the limiting phrase which was a legacy of the BSIG of 2009.[41] The operative phrase is now "security in the IT of *critical* infrastructures."[42]

An amendment to section 3 of the Act carried out the legislative purpose of having the BSI function as a threat sharing agency by permitting the sharing of intelligence with third parties.[43] Legislative materials elaborate that this

---

[39] *Functions*, BUNDESNETZAGENTUR, https://www.bundesnetzagentur.de/EN/General/Bundesnetzagentur/About/Functions/functions_node.html (last visited Dec. 16, 2017).

[40] A reader already familiar with the provisions might find fault with the priorities of the present selection. Moreover, one should not be tempted to conclude that a particular specific subject matter is left unregulated by the within law simply because it is not highlighted here.

[41] See *supra* note 19 and the accompanying discussion there.

[42] *Compare* the BSIG of 2009, *supra* note 11, *with* the IT Security Act *supra* note 31, no. 3.a)bb), at 1324. See also the associated discussion supra at note

[43] *Das BSI*, BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK,

provision was intended to extend not only to any other operator of critical infrastructure but to a very broad set of organizational types. Namely, threat intelligence could be shared with

> other facilities or businesses which, though not operators of critical infrastructure in terms of the BSIG, are nonetheless known to be part of Critical Infrastructure in the broader sense, or which otherwise have a justified security interest in the information in question (for example in the culture and media sector, which is not covered, or research organizations).[44]

Moreover, the BSI was made the central agency for IT security cooperation with competent agencies abroad, without prejudice to the competences of other German federal agencies.[45]

During the legislative process in 2015, the Bundesrat (the Federal Council) criticized certain terms in the proposed Act as too indefinite. In response, the government cited constitutional case law upholding the use of indefinite terms as unavoidable in light of many multifaceted, real-world circumstances.[46] The very dynamic nature of the cybersecurity field, argued the law's sponsors, meant concrete future developments could not be accounted for. Indeterminate legal terms were therefore supposed to preserve the relevance of the statute over time and make it

---

http://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz_node.html (last visited Mar. 5, 2018) (Ger.); BR 643/14, *supra* note 33, at 29.

[44] BR 643/14, *supra* note 33, at 29 (translation by the author).

[45] IT Security Act, *supra* note 31, no. 3.a)cc), at 1324.

[46] BT 18/4906, *supra* note 33, at 48 (Ger.) (internal citations to constitutional case law omitted).

tech-agnostic.[47]

The definition selected for "critical infrastructure" extended to facilities and installations or components thereof that were highly meaningful for the functioning of society because their failure or impairment would lead to severe shortages or endanger public safety.[48] The Act designated a list of critical sectors as critical in terms of securing the basic needs of citizens. These were the energy, IT and telecom, logistics and transportation, healthcare, water, food, and finance and insurance sectors.[49] Due to the complexity of determining what entities were subject to the Act, authority was delegated to the BSI to issue further regulations of critical infrastructures on the basis of ongoing consultations with affected persons, entities and experts.[50] (These regulations are addressed briefly below.)

The Bundestag also recognized that there was additional infrastructure qualitatively just as critical as what the Act addressed expressly. But the competence to regulate these other categories was not among its constitutionally enumerated powers. State and municipal governments, as well as entities in the culture and media sector, are examples of those that are left to German state law.[51] Federal government infrastructure belonging to the executive and legislative branches, on the other hand, does fall within the scope of the Act.[52]

The BSI's authorization to issue warnings was modified. The agency could now issue warnings either directly to the general public or only to those affected. It

---

[47] *Id.*
[48] IT Security Act, *supra* note 31, no. 2, at 1324.
[49] *Id.* no. 2.1.
[50] *Id.* no. 2.2; *see also* BT 18/4096, *supra* note 33 at 29.
[51] BT 18/4096, *supra* note 33 at 29.
[52] *Id.*

could warn of security flaws in IT products and services, malicious software, or loss of or unauthorized access to data. The BSI was permitted to bring in third parties where an effective and timely warning required it.[53] But most salient in the BSI's own view were new provisions requiring operators of critical infrastructure to demonstrate regularly, or at least every two years, that they are practicing state-of-the-art IT security. Paramount in the agency's view was also the authority to order remediation of deficiencies in conjunction with other regulators.[54] Operators were obligated to notify the BSI of any serious problems with their IT if the potential existed that critical services would be affected.[55] Regulated entities had six months to provide the BSI with a continuously available point of contact.[56]

This overview of the substance of the 2015 IT Security Act concludes by summarizing the parliamentary opposition's criticism of the legislation as enacted.[57] This is informative as to the realm of possibility—or at least as to the range of public sentiment at the time—beyond what the parliamentary majority eventually resolved to enact.

The oppositional parties proposed a resolution referring to Edward Snowden by name and recognizing a cybersecurity threat from state agencies, in particular Western intelligence agencies.[58] The view was that any

---

[53] IT Security Act, *supra* note 31, no. 5, at 1325.
[54] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, *supra* note **Error! Bookmark not defined.**.
[55] *Id.*; *see also* IT Security Act, *supra* note 31, at 1325-27.
[56] *Id.* at 1326.
[57] *See* Beschlussempfehlung und Bericht des Innenausschusses [Recommendation for resolution and report of the interior committee], June 6, 2015, BT 18/5121, 12-14, 17-18, http://dip21.bundestag.de/dip21/btd/18/051/1805121.pdf (Ger.).
[58] *Id.* at 12.

legislation ought to protect against violations of the citizens' fundamental right to confidentiality, as well as support the integrity of IT systems they use.[59] The new law ought to have contained additional provisions, it thought. Specifically, it should have paid more attention to proportionality in determining when personally identifiable information was permitted to be processed. The standard triggering cybersecurity incident reporting should have been stated more broadly than "serious disturbances." Mass data retention solely for the purpose of IT security should have been proscribed. Industrial competition around good IT security should have been better incentivized. Penetration testing for government and private IT systems ought to have been implemented. "State of the art" cybersecurity should have expressly included risk analysis. Sanctions for failure to follow security standards ought to have been more effective. Legal liability, *e.g.*, for negligent implementation of IT or failure to eliminate security flaws, ought to have been imposed. Immediate publication of threat data and security flaws coming to the BSI's attention ought to have been mandatory. End-to-end encryption, open-source hardware and software-based infrastructure and bug bounty programs ought to have been made the norm.

Since the foregoing list was not enacted into law, the practitioner is left to determine the relevance of the opposition's demands or the extent to which the law, as enacted, reasonably requires any of the above, though it was not spelled out in a specific provision as enacted.

[59] *Id.* at 12.

IV. THE NIS DIRECTIVE OF THE EUROPEAN UNION

A mere sketch of the NIS Directive[60] appears here as the background to the most recent amendment of the corresponding German statute, discussed hereafter. After the Bundestag passed the IT Security Act of 2015, the European Union issued a directive on the security of network and information systems (the "NIS Directive").[61] The European Parliament adopted the NIS Directive on July 6, 2016, to enter into force in August, 2017.[62] Member states have until May 9, 2018 to transpose the NIS Directive into national law[63] and until November 9, 2018 to identify operators of "essential services."[64] The Bundestag regards "essential services" as the equivalent of "critical infrastructure."[65] The

---

[60] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L 194) 59, 1 – 30, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN [hereinafter NIS Directive].

[61] *The Directive on Security of Network and Information Systems (NIS Directive)*, EUROPEAN COMMISSION, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (last visited December 10, 2017).

[62] Martin Schallbruch, *NIS-Richtlinie verabschiedet: schwierige Umsetzung für digitale Dienste*, CRONLINE (July 15, 2016, 6:06 a.m.), www.cr-online.de/blog/2016/07/15/nis-richtlinie-verabschiedet-schwierige-umsetzung-fuer-digitale-dienste/ (Ger.).

[63] *Id.*

[64] *Id.*

[65] Gesetzentwurf der Bundesregierung [Cabinet draft], Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union [Draft of an act to implement Directive (EU) 2016/1148 of the European Parliament and of the Council *etc.*], BT 18/11242, Feb. 20,

NIS Directive leaves it to EU member states to specify what the corresponding services or infrastructure are.

According to the European Commission, the legislation was intended to "boost the overall level of cybersecurity in the EU" by several means.[66] Member states are to establish computer security incident response teams (CSIRTs) as well as a national authority for network and information security, as a preparation for cybersecurity incidents. The NIS Directive envisions both long-term as well as incident-related information sharing and cooperation among member-state representatives, the European Commission and the European Union Agency for Network and Information Security ("ENISA").[67]

"Digital services," defined as online marketplaces, online search engines and cloud computing services, were deemed essential and made subject to the regulation.[68] The EU member state in which such a service maintains its head office shall have jurisdiction. But if a digital service were offered in the EU by a provider without an establishment of that kind, then the provider "shall designate a representative in the Union . . . established in one of those Member States where the services are offered . . . [and] be deemed to be under the jurisdiction of the Member State where the representative is established."[69]

2017, at 1 (Ger.), http://dip21.bundestag.de/dip21/btd/18/112/1811242.pdf.

[66] EUROPEAN COMMISSION, *supra* note 61.

[67] *See* NIS Directive, *supra* note 60, declaration (4), at 2 ("For that group to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of security of network and information systems in their territory.").

[68] *See supra* note 60, Annex III, at 30.

[69] *See supra* note 60, Chapter V, at 21, 23 (on digital service providers' obligations generally and Art. 18 on member states' jurisdiction specifically).

V. THE 2017 AMENDMENT TO THE BSIG

Subsequently to the NIS Directive, the Bundestag once more amended the BSIG to transpose the Directive into national law.[70] An EU directive sets mandatory goals or standards the means of achieving which are left up to the national (member-state) legislatures.[71] The proponents of this set of amendments to the BSIG considered that the provisions of the earlier IT Security Act on operators of critical infrastructure[72] in Germany were substantially equivalent to the call of the NIS Directive regarding "essential services"[73] in the EU. However, the parliamentary opposition formally renewed its concern that the verbal standard for mandatory reporting, namely "serious security incidents," left too much wiggle room. It urged that more had to be done to prevent intelligence agencies having any use of data collected under the BSIG.[74] It also renewed its call for heightened liability provisions to force critical infrastructure operators to invest in IT security.[75] The legislative

---

[70] Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union vom 23. Juni 2017 [An act to give effect to Directive (EU) 2016/1148], BGBL I, 40, 1885 – 1892 (Ger.).

[71] *See Regulations, Directives and Other Acts*, EUROPEAN UNION, https://europa.eu/european-union/eu-law/legal-acts_en (last visited February 20, 2018).

[72] *See* IT Security Act, *supra* note 31, § 2 (10).

[73] Beschlussempfehlung und Bericht des Innenausschusses [Recommendation for resolution and report of the Committee on Internal Affairs], Mar. 30, 2017, BT 18/11808, at 1, http://dipbt.bundestag.de/dip21/btd/18/118/1811808.pdf (Ger.).

[74] *Id.* at 11.

[75] *Id.* at 11-12.

committee that reviewed the cabinet draft prior to adoption of the 2017 amendments drew attention to internet-of-things (hereinafter "IoT") devices, demanding a system of voluntary certification and quality labeling as a way to communicate indirectly with consumers.[76] The committee criticized as insufficient the EU regulations on IoT device security and called upon the German federal government to work out the labeling issues in conjunction with stakeholders and the BSI. It believed the government should lobby the EU to provide mandatory IT security requirements for IoT devices marketed in the EU.[77] Observing that security could not be achieved unless device owners act reasonably, labeling was deemed an appropriate way to let reasonable consumer behavior begin fundamentally with the choice of device.[78]

Despite the criticism, the legislation that was eventually enacted conformed German national law to the NIS Directive. It updated definitions so as to subject digital services offered within the EU to regulation under the BSIG regardless of the operator's presence in the territory.[79] Quantitative thresholds would exempt smaller operators. Certain exceptions applied to online marketplaces depending on the locality where the parties would be deemed

[76] *See id.* at 8.
[77] *Id.*
[78] *Id.* at 11.
[79] *See* An act to give effect to Directive (EU) 2016/1148, *supra* note 70 at 1885; Gesetzentwurf der Bundesregierung [cabinet draft], Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union [Draft of an act to give effect to Directive (EU) 2016/1148], BT 18/11242, Feb. 20, 2017, at 34, http://dip21.bundestag.de/dip21/btd/18/112/1811242.pdf.

to have entered into the contract of sale.[80] "Search engines" for purposes of the regulation were limited to services permitting queries on arbitrary topics.[81] Cloud computing was so defined as to apply to a "broad palette" of computational services—servers, networks, storage, applications or others—that were scalable, elastic, and available to multiple users.[82] The BSI was permitted to provide more comprehensive technical expertise at the request of the German states than had been available under the prior law, which had not authorized assistance beyond law enforcement and state-owned IT.[83] The act also provided for mobile incident response teams (generally "MIRTs") with which the BSI could support other entities in recovering their IT systems in the event of cyberattack.

Several provisions of Chapter II, Annex 1 to the NIS Directive, related to the activity of MIRTs, are implemented through the insertion of a new section 5a of the BSIG. They provide that MIRTs may assist federal government agencies, operators of critical infrastructure generally, and others in exceptional circumstances. Some measures were supposed to make it more palatable for a private firm to engage a MIRT with respect to cost or the risk of incurring telecommunications secrecy violations.[84] Provisions related to Art. 15(2) of the NIS Directive (which lets authorities examine not only the results of an IT security audit but also the underlying findings) appear in section 8a, paragraphs (3) and (4).[85] Section 8b, paragraph 4 was amended to reflect that the verbal standard for mandatory reporting—a

[80] *Id.*
[81] *Id.*
[82] *Id.* at 36.
[83] *Id.*
[84] *Id.* at 39-40.
[85] *Id.* at 43.

"serious" incident—was to be applied in light of how seriously the event impacted the functionality of critical infrastructure. The seriousness of the event solely from the perspective of IT security would not be the basis for determining mandatory reporting.[86]

The BSI has made various materials available in English on its website.[87] More extensive materials are available in German.[88] The BSI publishes an extensive annual public service report on the status of IT security in Germany.[89]

VI. AGENCY REGULATIONS

The 2017 amendments to the BSIG of 2009 were published along with agency regulations promulgated by the BMI pursuant to section 10 paragraph 1 of the BSIG in consultation with numerous other agencies of the German federal government.[90] Prior to amendment, regulations already existed specifying what would count as a "facility,"

---

[86] *Id.* at 47.

[87] *The BSI*, BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html (last visited December 20, 2017).

[88] *IT-Grundschutz*, BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html (last visited December 20, 2017).

[89] The 2017 report can be accessed at *BSI-Lagebericht IT-Sicherheit*, BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html (last visited Dec. 20, 2017).

[90] Erste Verordnung zur Änderung der BSI-Kritisverordnung vom 21. Juni 2017 [First regulation to modify the BSI *Kritis*-Regulation], June 29, 2017, BGBL I, 40, at 1903-1922, *available at* BUNDESANZEIGER VERLAG, http://mobile.bgbl.de/ (Ger.).

an "operator" and a "critical service" and quantifying a "degree of service" (Ger. *Versorgungsgrad*) and various threshold values that would determine whether the BSIG applied to a given operation.[91] These were actually the second of two rounds of updates begun under the previous IT Security Act. The first round dealt with the sectors energy, water and sewer, food, and IT and telecom.[92] The second round applied to the sectors healthcare,[93] insurance and financial services[94] and shipping and transportation.[95] Adjustments to prior regulations on water and sewer services were included with the second round.[96] Generally the threshold values are quantities such as, for example, gigawatt hours per year for an electrical transmission grid, or billions of liters of output per year for potable water.[97]

VII. CYBERSECURITY AND THE NEW FEDERAL DATA PROTECTION ACT

In 2017, the Bundestag passed an act to repeal the Federal Data Protection Act of 2003[98] and implement the

---

[91] BSI-Kritisverordnung vom 22. April 2016 [BSI-KritisV] [Regulation on determining critical infrastructures under the BSIG], May 2, 2016, BGBL I, 20, at 958-969, as amended (Ger.), *available at* https://www.gesetze-im-internet.de/bsi-kritisv/index.html, § 1.
[92] *See id.*
[93] *Id.* § 6.
[94] *Id.* § 7.
[95] *Id.* § 8.
[96] *Id.* § 3.
[97] *See id.* (generally, various categories of annexes by sector with computation methods and formulas).
[98] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 [Federal Data Protection Act in the version promulgated on January 14, 2003], January 14, 2003, BGBL I, 3, at 66-88, as amended. An officially commissioned English translation of the

GDPR.[99] The new Federal Data Protection Act (the "BDSG") implements the directly binding[100] GDPR along with provisions of national law which are permitted under various savings clauses in the GDPR. It will take effect on May 25, 2018. As of this writing an English translation of the new BDSG is available on the website of the International Association of Privacy Professionals.[101]

A provision of the former Act implicates IT security law, and the provision is substantially intact in the new Act. Section 9 of the old BDSG provides:

> Technical and organization measures
>
> Public and private bodies processing personal data either on their own behalf or on behalf of others shall take the technical and organizational measures necessary to ensure the implementation of the provisions of this Act, in particular the requirements set out in the annex to this Act. Measures shall be required only if the effort

---

Act, reflecting amendments through 2009, can be accessed for the time being at www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html (last accessed Dec. 17, 2017).

[99] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 30. Juni 2017 [DSAnpUG-EU] [An act to adapt data protection law to the Regulation (EU) 2016/679 and to give effect to the Directive (EU) 2016/680), June 30, 2017, BGBL I, 44, 2097-2132 [hereinafter the new BDSG], Art. 8(1), second sentence.

[100] EUROPEAN UNION, *supra* note 71.

[101] *The German Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (English)*, IAPP, https://iapp.org/resources/article/the-german-act-to-adapt-data-protection-law-to-regulation-eu-2016679-and-to-implement-directive-eu-2016680-english/# (last visited December 17, 2017).

> involved is reasonable in relation to the desired level of protection.[102]

The Annex specifies that "[w]here personal data are processed or used automatically, the internal organization of authorities or enterprises is to be arranged in such a way that it meets the specific requirement of data protection."[103]

The referenced Annex to the former BDSG specified the ends to be achieved by organizational means. Thus, no particular measures were required, but whatever was done had to be "suited to the type of personal data or data categories to be protected."[104] Access and use of data processing systems by unauthorized persons was to be prevented.[105] Authorized persons should have no access to data beyond their specific authorization. Personal data should not be available for unauthorized reading, copying, modification or removal during processing, storage, transport or transmission.[106] The destination of any personal data transmission had to be ascertainable, as did the identity of any persons inputting, modifying or removing data. Data processing agents were required to follow the principal's instructions strictly.[107] Personal data had to be protected from accidental destruction or loss, with data collected for different purposes being capable of separate processing.[108] The Annex expressly encouraged the use of encryption.[109]

---

[102] Federal Data Protection Act in the version promulgated on January 14, 2003, *supra* note 98, § 9, at 74.
[103] Federal Data Protection Act in the version promulgated on January 14, 2003, *supra* note 98, annex to § 9, at 88, first sentence.
[104] *Id.* second sentence.
[105] *Id.* second sentence nos. 1, 2.
[106] *Id.* second sentence no. 3.
[107] *Id.* second sentence nos. 4 – 6.
[108] *Id.* second sentence nos. 7 – 8.
[109] *Id.* third sentence.

Compare Art. 32(1) GDPR (security of processing) to this provision, which calls for

> [t]aking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk . . . the [data] controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk . . . .[110]

Letters (a) – (d) itemize "pseudonymisation" and encryption, ensuring confidentiality, integrity and authenticity ("CIA") plus resilience, timely recovery of systems after a physical or technical incident, and a process for regularly testing, assessing and evaluating the effectiveness of technical measures.[111]

The legal standards for IT security of critical infrastructure under the NIS Directive and BSIG closely resemble those for security of data processing under the GDPR and new BDSG. In particular, though data protection and IT security of critical infrastructure are formally distinct subject matter, the respective standards both refer to the state of the art and require measures proportionate to the associated risk of a breach.[112] Section 8a paragraph 1 of the

---

[110] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 59, 1-30, http://eur-lex.europa.eu/eli/reg/2016/679/oj.

[111] *Id.* The rest of Art. 32, *i.e.*, paras. (2) – (4), refers to risk assessment, approval of codes of conduct and a certification mechanism, and control of natural persons acting under the authority of a data controller or processor.

[112] The corresponding provision of the new BDSG is at section 64

BSIG prescribes appropriate measures "not out of proportion to the consequences of a failure or disruption of an affected critical infrastructure." By comparison, appropriate measures are to be determined under section 64(1) of the new BDSG considering the state of the art, the cost of implementation, the type, extent, circumstances and purposes of data processing as well as the likelihood of incidence of a danger to the protected interests of the affected persons. The same norm calls for observance of the technical guidelines and recommendations of the BSI. Thus, when it comes to IT security in Germany and Europe, personal data is entitled to essentially the same level of protection as the potable water supply.

VIII. PROPOSED EU REGULATION OF CYBERSECURITY PRODUCT CERTIFICATION IN THE COMMON MARKET AND ENISA AS THE EUROPEAN CYBERSECURITY AGENCY

This country brief concludes by drawing attention to the recently published European Commission proposed regulation of cybersecurity products. One of the stated aims of the proposed regulation is to get ahead of the plethora of ICT (that's information and communications technology) devices on the horizon to achieve a high level of cybersecurity.[113] The proposal foresees making ENISA—

Anforderungen an die Sicherheit der Datenverarbeitung [Requirements for the security of data processing]. *See* the new BDSG, *supra* notes 99 (Ger.) & 101; *see also* SCHAFFLAND/WILTFANG, DS-GVO Art. 32 *Vorbemerkung* [preliminary remark] & paras. 4, 5, 140, *available at* WWW.DATENSCHUTZDIGITAL.DE by subscription (Ger.).

[113] *Commission Proposal*, *supra* note 9 (citing for instance connected and automated cars, electronic health systems and industrial automation control systems, or "IACS"). The proposed text of the regulation begins at p. 22.

the European Union's cybersecurity agency located in Greece—into a permanent agency with an expanded mandate. One mandate would be to establish sector-specific information sharing hubs called "Information Sharing and Analysis Centres."[114] ENISA would also oversee market-related tasks such as standardization and certification of products.[115] The aim is to avoid internal fragmentation of the single European market for cybersecurity product certification.[116] The proposed regulation and public comments are found on the website of the European Commission.[117] Around the same time the European Commission published this proposal, it also issued a recommendation on coordinated response to large-scale cybersecurity incidents and crises.[118]

[114] *Id.* at 4-7.
[115] *Id.* at 7.
[116] *See id.* at 9-10 & n.15.
[117] *See* Cybersecurity Package, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en (last visited Dec. 20, 2017).
[118] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises, C/2017/6100, O.J. (L 239) 60, 36 – 58, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H1584&from=EN.